November 2005

# PGP® Research Report – Summary

## National Survey on Data Security Breach Notification

Sponsored by the global law firm of

WHITE & CASE

Independently conducted by

Ponemon Institute LLC

Distributed with permission by PGP Corporation

PGP®

# Table of Contents

# National Survey on Data Security Breach Notification

## Recipients of Data Security Breach Notices Are Not Satisfied with Initial Communications

## Introduction

We are pleased to report results for our National Survey on Data Security Breach Notification. Survey fieldwork was completed on August 25, 2005. This perception-capture research was independently conducted to learn how individuals react to data security breach notifications sent by business, non-profit, or governmental organizations as required by new laws. The purpose of this study is to learn how organizations met their legal obligation to notify individuals after the loss or theft of personal information. In addition, this study seeks to understand how individuals reacted to the organization's communication and handling of this critical event.

Invitations were sent to 51,433 adult-aged individuals throughout the United States by email or letter. We received 9,154 usable Web-based survey responses from individuals residing in all major regions, resulting in a 17.8% response rate. Of these respondents, more than 11.6% or 1,109 individuals self-reported that they received communications from an organization about the loss or theft of their personal information.

## Executive Summary

The National Survey on Data Security Breach Notification addresses the notification practices of U.S.–based organizations in business and government when a data security breach occurs and personal information is either lost or stolen. In accordance with various new state laws and emerging U.S. federal regulations, organizations are required to notify victims of the breach in a timely fashion.

According to our research, individuals receiving the data breach notification tend to blame the organization for not having sufficient controls or safeguards to protect their data. Should the victims of the breach suffer such negative consequences as identity theft, our research further indicates that they are likely to lose trust and confidence in the organization. Obviously, lost trust will likely cause many customers to terminate their relationship with the organization ("turnover"), especially if they believe its response to and handling of the security breach is unsatisfactory.

All organizations are vulnerable to a data security breach. However, it seems that what determines an organization's ability to protect its reputation and maintain the trust of its customers and employees in the aftermath of a breach is the quality of the notification. For this reason, we have surveyed individuals who have been notified about a data security breach and asked them specific questions about the content and the process of the notification. The following findings are the most informative about our respondents' perceptions.

## Survey Findings

Data breach incidents appear to be a pervasive problem in the United States, becoming more transparent as a result of several new state privacy laws.

- Approximately 11.6% of survey respondents reported that they have received notification of a data security breach within the last year.
- Our study suggests that more than 23 million U.S. adult-aged residents recall receiving a breach notification.
- About 86% of security breaches involved the loss or theft of customer or consumer information. About 14% involved employee, student, medical, and taxpayer data.
- The most likely organizations to report a breach are banks, credit card companies, governmental organizations (including state universities), and health care providers.

A majority of respondents were not satisfied with the quality of the notification and communication process.

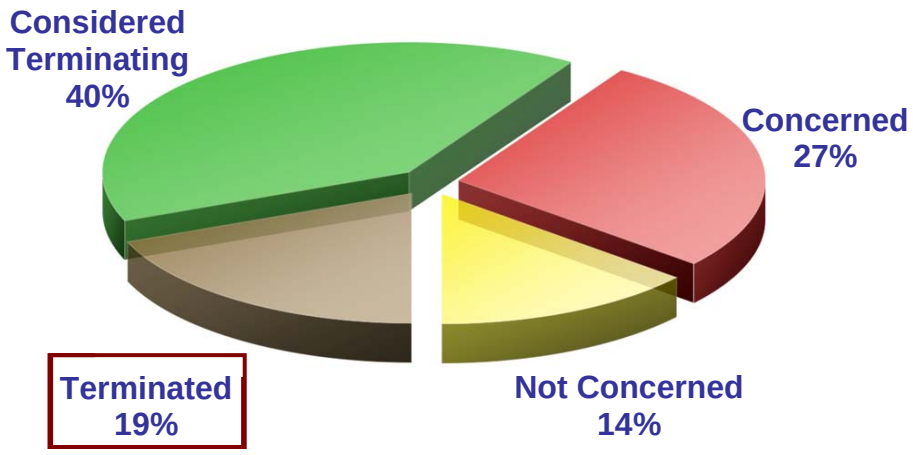
- Companies that report a breach to consumers are more than four times (417%) more likely to experience customer turnover if they fail to communicate to the victim in a clear, consistent, and timely fashion.
- Companies that deploy emails or form letters to communicate a breach of consumer data are more than three times (326%) more likely to experience customer turnover than companies that use telephone, personalized letters, or a combination of both.

People are fearful the data breach will have a significant negative impact on them and their families.

- More than 58% of respondents believed the breach decreased their sense of trust and confidence in the organization reporting the incident.
- More than 86% of subjects are concerned or very concerned about how data breach incident will affect them.
- Only 8% of respondents did not blame the organization that reported the breach.

**As a result, many notice recipients have lost trust and discontinued support for organizations reporting the incident.**

- **19% of respondents have already discontinued their relationship with the company as a result of the data breach.**
- **More than 40% said that they might discontinue their relationship.**
- **An additional 27% were concerned with the notifying organization.**
- **Only 14% of respondents replied they were not concerned.**




## Complete Report Available

If you have questions or comments about this research report or would like to obtain a full copy (including permission to quote or reuse the report), please contact by letter, phone, or email Ponemon Institute, LLC, Attn: Research Department, 212 River Street, Elk Rapids, Michigan 49629, 1.800.887.3118, research@ponemon.org.

## About the Study's Sponsor

**White & Case LLP** is a leading global law firm with nearly 1,900 lawyers in 38 offices in 25 countries. Our clients value both the breadth of our network and depth of our U.S., English and local law capabilities in each of our offices and rely on us for their complex cross-border commercial and financial transactions and for international arbitration and litigation. Whether in established or emerging markets, the hallmark of White & Case is our complete dedication to the business priorities and legal needs of our clients.

White & Case's Privacy Practice operates at the forefront of privacy issues and data protection laws. We advise clients on how to adopt sound privacy practices, avoid privacy risks, and protect their competitive advantage. We also represent clients in privacy-related litigations. Each year we host an annual symposium, regularly write articles, publish or sponsor surveys related to complex privacy issues. For more details, visit www.whitecase.com or contact Sandi Sonnenfeld, Media Relations Manager, at 1.212.819.8299 or via email at ssonnenfeld@whitecase.com.

## About Ponemon Institute, LLC

***Advancing Responsible Information Management***

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the Council of American Survey Research Organizations (CASRO), we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

## About PGP Corporation

The global customer standard for encryption and digital-signature solutions, PGP Corporation develops, markets, and supports an integrated data security suite used by more than 30,000 enterprises, businesses, and governments worldwide, including 84% of the Fortune® 100, 66% of the Fortune® Global 100, and thousands of individuals and cryptography experts. Customers depend on PGP solutions for regulatory and audit compliance, to protect confidential company information, to secure customer data, and to keep identity information private.

During the past 10 years, PGP® technology has earned a global reputation for innovative, standards-based, trusted solutions. The flexible PGP suite allows customers to phase-in gateway, partner, mobile or internal email security; data storage protection for laptops, desktops, and removable media; IM encryption; and FTP/batch transfer security using a single key management and recovery infrastructure. PGP Corporation is the only commercial security vendor to publish source code for peer review. Contact PGP Corporation at www.pgp.com or +1 650 319 9000.